SYSTEM AND METHOD FOR SECURE SMARTCARD ISSUANCE

This application claims priority from U.S. provisional application serial No. 60/224,994, filed August 14, 2000, entitled Signing Interface Requirements, Smart Card Compliance Requirements, Warranty Service Functional Requirements, and Additional Disclosure, which is hereby incorporated by reference.

BACKGROUND OF THE INVENTION

The world of electronic commerce has created new challenges to establishing relationships between contracting parties. One of those challenges springs from the fact that the parties to the transaction cannot see or hear each other, and cannot otherwise easily confirm each other's identity and authority to act.

One remedy for this problem is to provide each contracting party with a private key for signing transmitted messages with a digital signature. The signing party makes available an associated public key that decrypts messages signed with the party's private key, and thus enables a receiving party to confirm the identity of the sender.

The digital signature is typically created by a smartcard subsystem resident on the signing party's computer. This subsystem comprises a hardware token that stores the signing party's private key and any necessary software for executing the digital signature.

But the signature created by the smartcard is only as secure as the card's private key. It is therefore critical that the private key be protected from compromise by cryptographic or other attacks.

Many prior art electronic commerce systems, however, fail to adequately protect the private key from compromise. For example, some systems maintain more than one copy of the private key including one or more copies of the private key that may be maintained outside the card. If an unauthorized party gains access to one such copy, he or she can masquerade as the buyer. As a result, the buying parties cannot be assured that their signatures will not be affixed to unauthorized transactions and selling parties cannot be assured that a completed transaction will not later be refuted by the buying party. The failure to assure the security of a party's private key on the party's smartcard may thus compromise the ability of parties to conduct secure electronic commerce.

SUMMARY OF THE INVENTION

A system and method are disclosed for ensuring the security and integrity of a party's private key stored on a smartcard or other hardware token. A set of security

requirements are defined for the smartcard that ensure that the card is manufactured and initialized in a secure environment and that it can withstand certain types of cryptographic and other attacks. The requirements further ensure that, at the conclusion of the initiation process, there exists only a single instance of the private key which may never leave the smartcard. The unique existence of the private key in the smartcard allows the key to be treated as physical property and differentiates the key from other computer data which can be copied and allowed to proliferate.

In a preferred embodiment, the smartcard and private key are intended for use within the context of a four-corner trust model. This four-corner model preferably comprises a buyer, also referred to as the subscribing customer, and a seller, also referred to as the relying customer, who engage in an on-line transaction.

The four-corner model also preferably comprises a first financial institution, referred to as the issuing participant. The issuing participant acts as a certificate authority for the buyer and issues the buyer a hardware token including a private key and a digital certificate signed by the issuing participant.

The four-corner model also preferably comprises a second financial institution, referred to as the relying participant. The seller is a customer of the relying participant and accesses system services via systems maintained by the relying participant.

The system also includes a root certificate authority that issues digital certificates to the issuing and relying participants. The root entity is also preferably responsible for establishing the security requirements for smartcards issued by the issuing participant described above as well as interoperability requirements that ensure the interoperability of the hardware tokens with other system components.

The features and advantages described in the specification are not all inclusive, and many additional features and advantages will be apparent to one of ordinary skill in the art in view of the drawings, specification, and claims hereof.

BRIEF DESCRIPTION OF THE DRAWINGS

The above summary of the invention will be better understood when taken in conjunction with the following detailed description and accompanying drawings, in which:

FIG. 1 is a block diagram of a preferred embodiment of the four-corner model employed by the present system;

FIG. 2 illustrates certain components provided at relying customer 108 and subscribing customer 106 in a preferred embodiment of the present system;

FIG. 3 illustrates the components of a smartcard subsystem in a preferred embodiment of the present system;

FIG. 4A schematically illustrates the components of a smartcard token in a preferred embodiment of the present system;

FIG. 4B schematically illustrates the functional modules of a smartcard token in a preferred embodiment of the present system;

FIG. 5 illustrates a set of security requirements in a preferred embodiment of the present system;

FIG. 6 illustrates the relationship between a set of high-level security objectives and a set of low-level security requirements in a preferred embodiment of the present system;

FIG. 7 illustrates the relationship between a set of security-threat categories and a set of low-level security requirements in a preferred embodiment of the present system;

FIG. 8 illustrates a preferred embodiment of a process for generating an identity private key;

FIG. 9 illustrates a second preferred embodiment of a process for generating an identity private key;

FIG. 10 illustrates a preferred embodiment for using a smartcard to sign a digital message; and

FIG. 11 illustrates a preferred embodiment of weights assigned to requirements specified by root entity 110.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present disclosure relates to a system and method for manufacturing and initializing smartcards and other hardware tokens in a manner that ensures the security and integrity of information stored on the card. In a preferred embodiment, the smartcard is used by a signing party to sign digital messages relating to transactions conducted within the context of a four-corner trust model. A preferred embodiment of this four-corner model is shown in FIG. 1.

As shown in FIG. 1, the four-corner model preferably comprises a first institution 102 and a second institution 104. First institution 102 is referred to as the "issuing participant" because it is a participant in the present system and issues smartcards to its customers, as described below. Second institution 104 is referred to as the "relying participant" because it is a participant in the present system and its customers rely on representations made by issuing participant 102 and issuing participant 102's customers, as

described below. Participants 102, 104 may preferably be banks or other financial institutions.

Also shown in FIG. 1 are a first customer 106 and a second customer 108. First customer 106 and second customer 108 are preferably customers of issuing participant 102 and relying participant 104, respectively. First customer 106 is referred to as the "subscribing customer" because this customer subscribes to services provided by issuing participant 102. First customer 106 is also referred to as the "buyer" because it typically fills that role in transactions with second customer 108.

Second customer 108 is referred to as the "relying customer" because it relies on representations made by both issuing participant 102 and subscribing customer 106. Second customer 108 is also referred to as the "seller" because it typically fills that role in transactions with first customer 106. It should be recognized, however, that although the description below speaks primarily in terms of a buyer 106 and a seller 108, first customer 106 and second customer 108 may instead have different roles in a given transaction. For example, first customer 106 may be a borrower repaying a loan to second customer 108.

Also shown in FIG. 1 is a root entity 110. Root entity 110 is typically an organization that establishes and enforces a common set of operating rules for facilitating electronic commerce and electronic communications. Root entity 110 may be owned jointly by a plurality of banks and/or other financial institutions that have agreed to adhere to these operating rules. One exemplary embodiment of such a root entity is described in copending U.S. patent application serial No. 09/502,450, filed February 11, 2000, entitled System and Method for Providing Certification Related and Other Services and in copending U.S. patent application serial No. 09/657,623, filed September 8, 2000, entitled System and Method for Providing Certificate-Related and Other Services, which are hereby incorporated by reference.

In a preferred embodiment, the smartcard issued to subscribing customer 106 is provided with two private keys and corresponding digital certificates: an identity private key and corresponding certificate, and a utility private key and corresponding certificate.

The identity private key is used to produce digital signatures that are required by root entity 110 as evidence of an entity's contractual commitment to the contents of an electronic transaction, such as a purchase order or a warranty request such as the warranty request described in U.S. provisional application serial No. 60/224,994, filed August 14, 2000, entitled Signing Interface Requirements, Smart Card Compliance Requirements, Warranty Service Functional Requirements, and Additional Disclosure and U.S. application

serial No. _____, filed August 14, 2001, entitled System and Method for Providing Warranties in Electronic Commerce, which are hereby incorporated by reference.

The utility private key is preferably used to produce digital signatures that allow additional transactional security. Typically, utility certificates are used to support SSL, to sign S/MIME messages, and for other utility applications. Any reference in this document to a "certificate" refers to an identity certificate unless otherwise stated.

FIG. 2 illustrates components preferably provided at relying customer 108 and subscribing customer 106 in the present system. As shown in FIG. 2, relying customer 108 is preferably provided with a Web server 220 adapted to serve Web pages and other Web content via the Internet. Relying customer 108 is further preferably provided with a bank interface 222 for accessing services from relying participant 104. An exemplary bank interface is described in copending application serial No. 09/657,604, filed on September 8, 2000, entitled System and Method for Facilitating Access by Sellers to Certificate-Related and Other Services. Relying customer 108 is further preferably provided with a hardware security module 250 for executing and verifying digital signatures.

As further shown in FIG. 2, subscribing customer 106 is preferably provided with a Web browser 224 adapted to transmit requests for Web pages and other Web content via the Internet, and to receive responses to those requests. Issuing participant 102 is further preferably provided with a smartcard subsystem 226 for signing transaction data, described in further detail below. In a preferred embodiment, the components that make up smartcard subsystem 226 are provided to buyer 106 by its issuing participant 102.

In a preferred embodiment, subscribing customer 106 may also be provided with a signing interface (not shown). A preferred signing interface is described in U.S. provisional application serial No. 60/224,994, filed August 14, 2000, entitled Signing Interface Requirements, Smart Card Compliance Requirements, Warranty Service Functional Requirements, and Additional Disclosure and U.S. application serial No. _____, filed August 14, 2001, entitled System and Method for Facilitating Signing by Buyers in Electronic Commerce, which are hereby incorporated by reference. As described in that application, the signing interface provides a mechanism by which a seller's Web applications may invoke the buyer's smartcard subsystem or other signing module to execute a digital signature.

FIG. 3 illustrates a preferred embodiment of components included in smartcard subsystem 226. As shown in FIG. 3, smartcard subsystem 226 preferably comprises smartcard drivers and other software 310 ("drivers 310"), a smartcard reader 320 ("reader 320"), and a smartcard token 400.

Reader 320 and drivers 310 facilitate communication between smartcard token 400 and other software running on subscribing customer 106's computer system. Smartcard token 400 preferably comprises an integrated circuit card, such as an International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 7816 integrated circuit card. Alternatively, a personal security token, such as a Personal Computer Memory Card International Association (PCMCIA) device, or other comparable devices may be used.

In a preferred embodiment, smartcard token 400 is preferably owned by issuing participant 102 and made available for use to subscribing customer 106 under terms of a contract between subscribing customer 106 and issuing participant 102. In addition, as noted below, only a single instance of the subscribing customer's identity private key is permitted to exist once card-initialization is completed, and this instance of the key must be stored on smartcard token 400 and must never leave the card. Accordingly, the physical manifestation of the identity private key on smartcard token 400 shares an important characteristic of physical property (i.e., its uniqueness) that differentiates it from other computer data that may be copied and allowed to proliferate. Consequently, in a preferred embodiment, the contract with subscribing customer 106 further specifies that the physical manifestation of the private key is owned by issuing participant 102.

In an alternative embodiment, smartcard token 400 and/or the physical manifestation of the identity private key may be owned by root entity 110. In a second alternative embodiment, smartcard token 400 and/or the physical manifestation of the identity private key may be owned by subscribing customer 106.

FIG. 4A illustrates a preferred embodiment of smartcard token 400. As shown in FIG. 4A, smartcard token 400 preferably comprises a chip 401 that comprises a processor 405, a memory 410, and an I/O module 415. Processor 405 preferably runs a high-security multi-application operating system, such as MULTOS.

In a preferred embodiment, processor 405 is programmed to perform various functions including those shown as functional modules in FIG. 4B. As shown in FIG. 4B, one such module is a signature generator 424. Signature generator 424 is adapted to generate a digital signature using either the identity private key or utility private key, depending on the nature of the message to be signed. Signature generator 424 preferably generates RSA-based digital signatures using 1024 bit keys based on the RSASSA-PKCS-v 1_5 signature scheme and the SHA-1 with RSA encryption method.

Also shown in FIG. 4B are two counters 422 and 423. Counter 422 monotonically increases each time smartcard token 400 generates a signature using the identity private key.

Counter 423 keeps track of the number of consecutive failed attempts to enter subscribing customer 106's personal identification number (PIN)/passphrase before the identity private key is blocked, as discussed below.

CSSD generator 426 generates card and signature security data (CSSD) that may be included in signed transaction data to provide additional security, such as protection against duplicate message submission. In a preferred embodiment, root entity 110 does not impose any requirements concerning CSSD. Rather, issuing participant 102 determines whether and what type of CSSD to require as part of its risk management process.

CSSD is preferably generated using an authentication algorithm and a key. If the key used is the subscriber's identity private key, CSSD generator 426 preferably uses a different algorithm to generate the CSSD cryptogram than the algorithm used to sign the transaction data itself in order to avoid potential attacks on smartcard token 400. Thus, for example, if the algorithm used by smartcard subsystem 226 to generate signatures with the subscriber's identity private key is SHA-1 with RSA signature, then CSSD generator 426 preferably uses a different algorithm to generate CSSD cryptograms. This different algorithm preferably has a strength greater than or equal to 1024 bit RSA.

In a preferred embodiment, a hash of the transaction data to be signed is included as part of the authenticated data within the CSSD data block.

Smartcard token 400 may also comprise additional applications 425, i.e., applications that provide functionality not required to conduct transactions or obtain services within the four-corner model. In a preferred embodiment, such applications must nevertheless comply with security requirements for smartcard token 400 specified by root entity 110, as described below. In addition, such applications preferably do not use or have access to secure data on smartcard token 400, such as subscribing customer's 106 identity private key and PIN/passphrase.

In some embodiments, smartcard token 400 may also comprise a key generator 421 adapted to generate private/public key pairs, as described below.

A preferred set of functionality requirements for smartcard token 400 is now described. These functionality requirements are preferably specified by root entity 110 to facilitate interoperability of the subscribing customer's smartcard with other system components.

1. Smartcard token 400 must be adapted to create signatures using SHA-1 and RSA with 160-bit HASH Keys (as described in PKCS #1 v 1.5)

2. Smartcard token 400 must be adapted to use signature scheme RSASSA-PKCS-vl_5.

3. Smartcard token 400 must be adapted to store securely the subscriber's utility private key and identity private key in accordance with PKCS #1 v 2.0.

4. Smartcard token 400 must be adapted to store securely a cardholder PIN of at least six numeric characters, although a passphrase of at least 8 ASCII characters is recommended.

5. If implementing the security officer functionality (described below), smartcard token 400 must be adapted to store securely a security officer PIN/passphrase of at least six numeric characters, although a passphrase of at least 8 alphanumeric characters is recommended..

6. If required by issuing participant 102, smartcard token 400 must be adapted to store securely CSSD specified by the issuing participant. CSSD is a mechanism used to provide additional security (such as protection against duplicate message submission) for digital messages.

7. If CSSD is implemented on smartcard token 400, then the card must be adapted to implement an internal counter value that monotonically increases each time the identity key is used to generate a signature.

8. If CSSD is implemented on smartcard token 400, then the card must be adapted to use an authentication algorithm and key to generate the CSSD cryptogram. If the Key used is the identity private key, then the signature algorithm must not be SHA-1 with RSA signature. Other algorithms may be used, but must have strength equivalent to or greater than 1024 bit RSA. In other words, the algorithm used to generate the CSSD signature must be different than the one used to sign digital messages in order to avoid potential attacks.

9. If CSSD is implemented on smartcard token 400, then the card must be adapted to implement a mechanism for ensuring that the transaction hash (i.e., the data sent to the buyer for signature) is part of the authenticated data within the CSSD block.

10. Smartcard token 400 must be adapted to generate RSA-based digital signatures using 1024 bit keys based on the following signature scheme and method:

Signature scheme: RSASSA-PKCS-vlj (Reference PKCS #1 v 2.0).

Method: SHA 1 with RSA encryption (Reference PKCS #1 v 2.0).

In a preferred embodiment, root entity 110 establishes security requirements for smartcard token 400 to ensure that the card functions properly and that the confidentiality and integrity of sensitive information that it stores are maintained. The security

requirements preferably include functional security requirements, hardware security requirements, and compliance requirements.

Functional Security Requirements

A preferred embodiment of the functional security requirements is as follows:

1 General

1. Smartcard token 400 must support the functionality necessary to comply with requirements established by root entity 110.

2. Smartcard token 400 must be adapted to ensure the proper functionality of all applications approved by root entity 110 for system use.

2 Manufacturing

1. The integrity of smartcard token 400 must be ensured during all manufacturing phases. The manufacturer must supply necessary information to prove that all reasonable precautions to ensure the integrity of smartcard tokens during all manufacturing phases have been taken.

2. The life-cycle data of smartcard token 400 must be documented by the manufacturer.

3. The life-cycle status of smartcard token 400 must be irreversible, i.e., it must not be possible to erase the card and start the personalization again, unless all private-key material from a first personalization can be completely erased so that it cannot be recovered before, during, or after the second personalization.

4. Sensitive data, including the identity and utility private keys, generated outside smartcard token 400 must be loaded in smartcard token 400 using 2-Key 3-DES encryption or alternative of equal strength.

5. The card personalizer must implement a key management scheme that ensures the confidentiality of sensitive data during the personalization process of smartcard token 400. The personalization process includes key generation, key loading, and loading of applications, including confidential data.

6. The card personalizer must verify the integrity of smartcard token 400 before personalization.

7. The manufacturing and personalization (initial private key loading or issuer specific data) of smartcard token 400 must take place in a production environment, that must prevent that:

a. secret data are compromised during the personalization process,

b. the personalization process is carried out incorrectly or illegally,

c. unauthorized software or data is loaded in smartcard token 400,

d. unauthorized personnel have access to the personalization area and equipment,

e. smartcard tokens are lost or stolen before and after personalization.

8. Trusted personnel must be appointed for personalization of smartcard token 400, responsible for:

a. key generation

b. key loading

c. loading software and confidential data

9. Dual control must be maintained during personalization for:

a. key generation

b. key loading

c. software and data loading

3 Private Keys

1. Both the identity private key and the utility private key must be stored on smartcard token 400.

2. All operations involving private keys must be performed on smartcard token 400. Smartcard token 400 must not support the export of any private key in any form whatsoever. Consequently, private keys, once injected into smartcard token 400, will exist only on that smartcard and will not be stored in any other location.

4 User PIN/Pass phrase

1. PINs or passphrases must be stored on smartcard token 400.

2. All operations involving a PIN or passphrase must be performed on smartcard token 400. Smartcard token 400 must not support the export of secret data (PIN/Passphrase) in any form whatsoever.

3. Smartcard token 400 must require an eight character minimum PIN/passphrase for a user to access the identity private key.

4. Initial user PIN/passphrase selection must be based upon a random character selection algorithm to reduce the likelihood of similar initial user PIN/passphrases in multiple smartcards. The card issuer must be required to use a different initial user PIN/passphrase for each card. To support the use of secure PIN pads it is acceptable for all eight characters to have numeric values.

5. The user must be required to set his or her PIN/passphrase before performing any operations using the identity private key.

6. If the issuing participant has set an initial PIN/passphrase for smartcard token 400, smartcard token 400 must check that the user-supplied value is different from that set by the issuing participant. If the two values are the same, smartcard token 400 must reject the attempted change.

7. Smartcard token 400 must provide an unambiguous association between the PIN/passphrase and the creation of an identity signature. Therefore:

a. the PIN/passphrase used to unlock the identity private key for purposes of applying an identity signature must not be used for any other purpose.

b. the PIN/passphrase must be provided by the user each time the identity private key is used. An identity private key can only be unlocked to generate a single identity signature.

5 Security Officer's PIN/Passphrase (optional, but if not implemented, card unblocking must be disabled)

1. Smartcard token 400 must enforce a six numeric-character minimum for the security officer PIN/passphrase. An eight character alphanumeric passphrase is recommended. (In an alternative preferred embodiment, an eight character alphanumeric passphrase may be required.)

2. Smartcard token 400 must not allow itself to be unblocked more than six times (see section 6 below re: card blocking/unblocking).

3. Security officer PIN/passphrase selection must be based upon a random character selection algorithm to reduce the likelihood of similar security officer PIN/passphrases in multiple smartcard tokens. The card issuer must use different security officer PIN/passphrases for each card. A smartcard token must contain no more than six security officer PIN/passphrases. Collectively, the PIN/passphrases must be adapted to allow no more than six unblocking operations. Thus, for example, smartcard token 400 may store one security officer PIN/passphrase which may be used up to six times or at most six security officer PIN/passphrases which must each be used at most once, i.e., for one unblocking operation.

4. It must not be possible to change the security officer PIN/passphrases once smartcard token 400 has been personalized. If a security officer changes or leaves, a new card must be issued, unless it can be demonstrated that the security officer does not know the unblock PIN.

5. The security officer must not have access to user PINs/passphrases. The security officer's role and the user's role must not be performed by the same person.

6. If a smartcard token 400 has been blocked due to a suspected or actual compromise of the PIN/passphrase, then new user PIN/passphrase assigned when unblocking the card must be different from the old user PIN/passphrase.

6 Blocking/unblocking

1. Smartcard token 400 must enforce a limit on the number of consecutive incorrect PINs/passphrases that it will allow before blocking the card (reversibly, if card unblocking is supported). This limit must be no greater than five. Note: If a correct PIN/passphrase is entered before the limit is exceeded, counter 423a which enforces this limit is reset.

2. When smartcard token 400 is in a "reversibly blocked" state, it must render inaccessible all applications that call for use of the identity private key. It is acceptable - although not required - for the utility private key to remain useable.

3. Once a card is reversibly blocked, it must be unblocked only by a secure mechanism under the control of the issuing participant. This secure mechanism may be a security officer PIN/passphrase, but others (such as secure messaging as used in EMV) are also acceptable if implemented in accordance with this requirement.

4. Smartcard token 400 shall enforce a limit of six unblocks. Once a card has hit that limit, the operational data and functions on the card must be permanently inaccessible (i.e. the card must be rendered irreversibly blocked).

7 Multi Application

1. All applications residing on smartcard token 400 must comply with the security requirements established by root entity 110.

2. Any applications residing on smartcard token 400 must not influence the correct behavior of any other application on smartcard token 400.

3. The identity private key, the utility private key, and any PIN/passphrases shall only be used by applications used to conduct transactions or obtain services within the four-corner model.

4. Every application that resides on smartcard token 400 must be certified against potential security flaws either through the underlying operating system (MULTOS) certification or by other means.

8 Key generation

1. Private key generation must only be performed during personalization of smartcard token 400. In many cases, key generation occurs before personalization. In this context personalization is taken to mean the whole process of key generation and binding of user to card. In particular, key generation can take place as a separate activity before binding the user to the card.

2. If smartcard token 400 supports key generation, it shall use a built-in hardware random number generator that passes either the statistical random number generator tests defined in FIPS 140-1, section 4.11.1, or alternative tests that provide equivalent or superior randomness checking.

3. If smartcard token 400 does not support key generation, then keys generated outside smartcard token 400 must be loaded on smartcard token 400 using 2Key 3-DES encryption alternative of equivalent strength. Only Utility keys may be escrowed by a trusted agent. The identity private key must not be escrowed or retained. It must be destroyed after personalization and may only exist in one unique smartcard token.

4. Keys generated outside smartcard token 400 must be generated by a hardware security module, complying with the specifications set forth in U.S. provisional application serial No. 60/153,203, filed September 10, 1999, entitled System and Process for Certification in Electronic Commerce, which was converted into co-pending U.S. patent application serial No. 09/657,605, filed September 8, 2000, entitled System and Method for Providing Certificate Validation and Other Services, both of which are hereby incorporated by reference.

As noted in functional security requirement 1.1 above, smartcard token 400 must support the functionality necessary to comply with requirements established by root entity 110. For example, root entity 110 may establish as a requirement that the smartcard operating system must check the appropriateness of private key usage before using a private key in a cryptographic operation and that (1) the identity private key must not be used for encryption/decryption, and (2) the utility private key must not be used for executing digital signatures. In that event, smartcard token 400 and its operating system must be adapted to enforce these requirements in order for the smartcard token to comply with functional security requirement 1.1 above.

Hardware Security Requirements

In a preferred embodiment, the hardware security requirements are defined in terms of security levels specified by root entity 110. FIG. 5 illustrates a preferred set of security

levels that may be specified by root entity 110. As shown in FIG. 5, root entity 110 preferably specifies two security levels: a "high" security level and a "beyond practicality" security level. These security levels are further defined in terms of the amount of time it would take to (a) prepare and (b) conduct an attack on smartcard token 400 under a variety of scenarios. Each scenario is defined in terms of an attacker and the equipment used by the attacker, as described below.

One potential attacker is called an "expert." Experts are persons who are familiar with the underlying algorithms, protocols, hardware, structures, and security principles and concepts implemented in smartcard token 400, and are capable of effectively using professional and specialized equipment (defined below).

Another potential attacker is a "proficient person." Proficient persons are also knowledgeable in that they are familiar with the security behavior of smartcard token 400. They are capable of effectively using domestic equipment and professional equipment, but not specialized equipment.

One class of equipment that may be used in conducting an attack is "domestic equipment." Domestic equipment is equipment that is readily available within the end user's operational environment, is a part of the smartcard subsystem itself, or can readily be purchased. Domestic equipment includes basic electronic equipment, standard personal computers, and simple and readily available analysis equipment (e.g. voltage meters).

Another class of equipment that may be used in conducting an attack is "professional equipment." Professional equipment is equipment that is not readily available to the public because (1) the equipment is expensive to the point that only facilities such as universities, reverse engineering labs, and chip fabricators typically have this equipment, and (2) the use of the equipment requires special skills or resources. Professional equipment includes logic analyzers, workstations, and probe stations.

Another class of equipment that may be used in conducting an attack is "specialized equipment." Specialized equipment is equipment that is not readily available to the public because (1) the equipment is very expensive and, (2) the equipment is so specialized that its distribution is controlled or restricted. Specialized equipment includes special code breakers, focused ion beam systems, and scanning electron microscopes.

An attack is an attempt by an adversary to obtain or modify sensitive information or services for which the attacker is not authorized. An attack comprises two phases:

A. the preparation phase during which the attack is developed such that the attack can be performed as efficiently as possible, and

B. the repeat attack phase during which the previously developed attack is performed on one device.

Returning to FIG. 5, for a system component to satisfy a "beyond practicality" security level established by root entity 110, it must be infeasible for either an expert or proficient person to prepare an attack against the component using domestic equipment, it must take at least six months for an expert and 12 months for a proficient person to prepare such an attack using professional equipment, and it must take an expert at least three months to prepare such an attack using specialized equipment. In addition, it must be infeasible for either an expert or proficient person to mount a previously prepared attack against the component using domestic equipment, it must take at least one month for an expert and three months for a proficient person to mount such an attack using professional equipment, and it must take an expert at least one week to mount such an attack using specialized equipment.

As further shown in FIG. 5, for a system component to satisfy a "high" security level established by root entity 110, it must take at least six months for an expert and 12 months for a proficient person to prepare an attack against the component using domestic equipment, it must take at least one month for an expert and six months for a proficient person to prepare such an attack using professional equipment, and it must take an expert at least one week to prepare such an attack using specialized equipment. In addition, it must take an expert one month and a proficient person three months to mount a previously prepared attack against the component using domestic equipment, it must take at least one week for an expert and one month for a proficient person to mount such an attack using professional equipment, and it must take an expert at least one day to mount such an attack using specialized equipment. As will be recognized, alternative security levels and corresponding definitions may be established.

In a preferred embodiment, root entity 110 first establishes a set of high-level security objectives for ensuring the security and integrity of smartcard token 400. Low-level requirements are then defined that specify the particular steps that will be taken to satisfy the high-level objectives. In addition, root entity preferably identifies known threats to the security and integrity of smartcard token 400 and ensures that these threats are adequately addressed by the low-level requirements. As new threats develop, root entity 110 may revise the low-level requirements; the high-level objectives, however, preferably do not change.

A preferred set of high-level security objectives for smartcard token 400 are as follows:

1. It is beyond practicality to breach the confidentiality of the identity private key and the utility private key.

2. It is beyond practicality to breach the confidentiality of the PIN/passphrase stored on smartcard token 400.

3. It is beyond practicality to change the life-cycle status of smartcard token 400.

4. It is beyond practicality to breach the integrity of the counters associated to smartcard token 400's blocking and unblocking mechanisms.

5. It requires a high security level attack to breach the confidentiality and/or integrity of smartcard token 400's data and program structures.

6. It requires a high security level attack to breach the integrity of the bond between the identity of the cardholder and smartcard token 400.

7. It requires a high security level attack to breach the integrity of root entity applications present at smartcard token 400.

8. It requires a high security level attack to breach the integrity of smartcard subsystem 226.

As noted, once root entity 110 has defined an appropriate set of high-level objectives, it defines a set of low-level security requirements to address them. A preferred set of low-level security requirements for smartcard token 400 is as follows:

Reverse Engineering and Chip Modifications

1. It is beyond practicality to remove layers on top of the smartcard chip surface without damaging the chip.

2. It requires a high security level attack to visualize the contents of read only memory (ROM) memory cells, including electrically erasable programmable read only memory (EEPROM) cells.

3. It is beyond practicality to reverse engineer the functionality of smartcard token 400.

4. It is beyond practicality to modify chip structures by means of an FIB system.

5. It is beyond practicality to modify individual memory cells.

6. It requires a high security level of attack to misuse the smartcard chip's test features.

7. It requires a high-level security attack to modify the smarcard chip's fuses.

8. It requires a high-level security attack of attack to modify or disable chip 401's security sensors.

Internal Attacks (probing)

9. It is beyond practicality to use a probing attack to retrieve information from smartcard token 400.

10. It requires a high security level of attack to change the status of the memory of smartcard token 400 via active probing techniques.

11. It requires a high security level attack to influence the correct functionality of logical building blocks at smartcard token 400 by means of active probing techniques.

12. It requires a high security level attack to influence the correct execution of applications approved by root entity 110 at smartcard 400 by means of active probing techniques.

13. It requires a high security level of attack to influence the correct programming of memory cells by means of active probing attacks.

14. It requires a high security level attack to obtain information from smartcard token 400 via voltage contrast.

External Attacks

15. It is beyond practicality to obtain sensitive information from smartcard token 400 by analyzing externally available information, such as the power consumption profile or timing analysis of critical processes on smartcard token 400.

16. It is beyond practicality to influence the correct execution of applications approved by root entity 110 on smartcard token 400 by disturbing external parameters such as the clock input, the temperature, or the power supply.

17. It is beyond practicality to obtain sensitive information by disturbing external parameters of smartcard token 400.

18. It requires a high security level attack to change the status of memory 410 by means of disturbing external parameters of smartcard token 400.

Root entity 110 preferably creates a matrix, such as that shown in FIG. 6, to demonstrate that each high-level security objective is addressed by at least one low-level security requirement. As will be recognized, alternative low-level objectives and matrixes may be established.

Root entity 110 also preferably identifies a set of potential security threats to smartcard token 400 and ensures that the low-level requirements described above adequately address the identified threats. In a preferred embodiment, root entity identifies the following potential security threats to smartcard token 400.

1. Chip modification. Chip modification may be accomplished by devices such as focused ion beam (FIB) systems that expose the surface of chip 401 and allow an attacker to

view and modify the contents of memory cells on smartcard token 400. FIB systems may also be used to make chip modifications in order to aid other attacks or to change the functionality of chip 401.

2. Reverse engineering. Reverse engineering may also be accomplished using FIB systems. If any of smartcard token 400's components are reverse engineered, it may be possible to derive the functionality of those components. Knowing the functionality, an attacker may be able to retrieve sensitive information from smartcard token 400.

3. Restoration of testing hardware and software. Before smartcard token 400 leaves the manufacturer, the testing hardware and software is preferably irreversibly deactivated. But if an attacker succeeds in restoring these test features by reactivating hardware fuses on chip 401, the attacker may be able to gain access to the smartcard's sensitive information.

4. Internal attack. An internal attack involves placing small probing needles on certain, critical nodes on the surface of the smartcard's chip. There are two types of probing attacks: a passive probing attack and an active probing attack. A passive probing attack involves tapping sensitive information from the chip's nodes. An active probing attack involves changing the information on these nodes. Thus, an active probing attack may be used to change the status of memory 410, change the programming of memory 410, or change the functionality of smartcard token 400.

5. External attack. External attack techniques include, without limitation, (a) simple power analysis (SPA), (b) differential power analysis (DPA), and (c) manipulation of the smartcard environment.

(a) SPA involves measuring the power consumption over time of smartcard token 400 while it is performing a cryptographic calculation. This measurement is called the power profile and can serve as a fingerprint of the processes running on smartcard token 400. In some cases, it may be possible to discover from this profile the algorithms used on smartcard token 400 as well as sensitive information generated by those algorithms.

(b) DPA involves recording a relatively large number of power traces on smartcard token 400. By statistically analyzing these traces, an attacker may be able to reverse engineer the algorithms running on the smartcard and hence determine a subscriber's private key.

(c) Manipulation of the smartcard environment involves suddenly varying some aspect of the smartcard's environment to affect the card's operation. For example, sudden variations in the token's voltage supply may slow the response of the token's internal reference signals, and may cause these signals to be misinterpreted by the token's internal busses which transport instructions and data during card operation and thus change

the functionality of applications running on the smartcard. Sudden variations in the token's clock signal or temperature extremes may also cause erratic behavior. These variations may change the correct execution of applications on the token, expose sensitive information, or change the token's memory status.

Root entity 110 preferably creates a matrix to demonstrate that each identified potential threat is addressed by at least one low-level objective. In doing so, it may generalize the above-identified threats into categories. A preferred set of threat categories are as follows: (1) direct reading of memory contents; (2) ability to retrieve hardware functionality; (3) changing hardware functionality; (4) tapping or reading internal information; (5) changing internal information; (6) changing logical functionality; and (7) information leakage. FIG. 7 graphically illustrates a preferred matrix between the low-level security requirements and security threat categories listed above. As will be recognized, other alternative threat categories and matrixes may be established.

Compliance Requirements

Root entity 110 preferably requires an independent third-party security evaluation of smartcard token 400. The security evaluation ensures that smartcard token 400 conforms with the security requirements established by root entity 110 and that it does not have hidden vulnerabilities.

In a preferred embodiment, this evaluation may be conducted in accordance with one or more of the following standards: the Information Technology Security Evaluation Criteria (ITSEC), the Common Criteria for Information Technology Security Evaluation (CC), the Federal Information Processing Standard (FIPS), the European Electronic Signature Standardization Initiative (EESSI), and the Visa Open Platform Certification. Alternatively, root entity 110 may develop its own standards.

If ITSEC is used to conduct the security evaluation, then smartcard token 400 preferably meets or exceeds ITSEC assurance level E4 with strength of mechanism "high." If CC is used, then smartcard token 400 preferably meets or exceeds CC assurance level EAL4+ with strength of function "high." If FIPS is used, then smartcard token 400 preferably meets or exceeds FIPS assurance level 2. If EESSI is used, then smartcard token 400 preferably meets or exceeds a level of compliance equivalent to CC EAL4+. If Visa Open Platform certification is used, then smartcard token 400 preferably meets or exceeds an assurance level comparable to those identified above. Regardless of the standard used, however, if there is a conflict between the standard and a policy or procedure established by root entity 110, then root entity 110's policies and procedures preferably control.

Root entity 110 may require a statement from issuing participant 102 certifying that each smartcard token 400 it issues complies with one of the above-listed standards. In addition, root entity 110 may require that issuing participant 102 issue a statement that its card issuance procedures, personalization procedures, and smartcard tokens ensure non-repudiable signatures. Issuing participant 102 typically satisfies this requirement by supplying documentation from accredited testing laboratories. Equivalent statements from smartcard vendors may also be used. In a preferred embodiment, smartcard tokens that are not certified may not be used in any transactions conducted within the four-corner model.

In a preferred embodiment, the degree of rigor required for the testing of smartcard token 400 may differ if the smartcard subsystem implements only applications used to conduct transactions or obtain services within the four-corner model, as opposed to a case where other applications are supported. In the latter case, it must be shown that the smartcard's operating system (such as MULTOS) is isolated from such other applications to such an extent that the applications can be evaluated independently of the operating system. If this is not the case, then additional evaluation and testing may preferably be required.

As a further measure of security, the integrity of smartcard token 400 is preferably ensured during all phases of the token's life-cycle. Smartcard token 400's life cycle includes chip fabrication, module fabrication, card manufacturing, card personalization, card distribution, card activation, and card termination. The manufacturing phase of the hardware token 400's life-cycle is preferably documented by the manufacturer. Manufacturers may be required to supply issuing participant 102 with proof that all reasonable precautions have been taken to ensure the integrity of smartcard token 400.

As noted, in a preferred embodiment, smartcard token 400 may be accessed by a security officer employed or authorized by issuing participant 102. The security officer verifies proper functionality and security of the components at smartcard token 400 but preferably is not given access to sensitive data stored on hardware token 400, such as subscriber 106's identity private key and PIN/passphrase. The security officer is preferably provided with a PIN/passphrase for unblocking smartcard token 400, as described above. Smartcard token 400 may store as many as six security officer PIN/passphrases.

In a preferred embodiment, issuing participant 102 is responsible for personalizing each smartcard token that it issues for a particular issuing participant 106. Issuing participant 102 preferably ensures that smartcard token 400 is personalized in an environment that prevents the identity private key from being compromised during personalization. The personalization environment also preferably prevents incorrect or illegal personalization, unauthorized software or data from being loaded onto the token,

unauthorized personnel from having access to the personalization area and equipment, and tokens from being lost or stolen before or after personalization.

FIG. 8 illustrates a preferred embodiment of a smartcard token personalization process in which an identity private key is generated on smartcard token 400. As shown in FIG. 8, in step 801, issuing participant 102 verifies the integrity of smartcard token 400. This step may include, for example, examining appropriate documentation from the vendor that manufactured smartcard token 400 that confirms that the token was manufactured in accordance with suitable security standards. In step 802, key generator 421 generates an identity private key and its corresponding public key. In step 803, the identity private key is stored in memory 410. In step 804, key generator 421 generates a utility private key and its corresponding public key. In step 805, the utility private key is stored in memory 410. Smartcard token 400 is preferably adapted to prevent any export of either private key from smartcard token 400.

In step 806, any desired additional software and data are loaded onto smartcard token 400. In step 807, issuing participant 102 binds subscribing customer 106 to smartcard token 400 by verifying subscribing customer 106's identity and creating a digital certificate for the subscribing customer that includes the customer's identity public key. In step 808, issuing participant 102 physically issues the smartcard containing the subscribing customer 106's private key to the subscribing customer.

In step 809, issuing participant 102 provides subscribing customer 106 a copy of the customer's digital certificate. In a preferred embodiment, the certificate is not stored on the subscriber's smartcard token 400. This increases system security because if the smartcard token is lost or stolen, the finder will not be able to determine the subscriber's identity from the smartcard and will therefore find it difficult or impossible to forge digital signatures in the subscriber's name. In this preferred embodiment, the subscriber's certificate is preferably delivered to the subscriber on some other medium or by electronic transmission and then stored in a personal security environment (PSE) outside the token. In an alternative embodiment, the subscriber's certificate may be stored on smartcard token 400.

FIG. 9 illustrates a preferred embodiment of a smartcard token personalization process in which the identity private key is generated outside the card. As shown in FIG. 9, in step 901, issuing participant 102 verifies the integrity of smartcard token 400, as described above. In step 902, issuing participant 102 generates an identity private key and a corresponding public key. In step 903, issuing participant 102 generates a utility private key and a corresponding public key. As noted, these private keys are preferably generated using a hardware security module that complies with requirements specified by root entity 110.

An exemplary set of hardware security module requirements are set forth in U.S. provisional application serial No. 60/153,203, filed September 10, 1999, entitled System and Process for Certification in Electronic Commerce, which was converted into co-pending U.S. patent application serial No. 09/657,605, filed September 8, 2000, entitled System and Method for Providing Certificate Validation and Other Services, both of which are hereby incorporated by reference.

In step 904, the private keys are loaded onto smartcard token 400. As noted, the private keys are preferably loaded onto the token with at least 2-Key 3-DES encryption via a key management system which ensures the confidentiality and integrity of the private keys during the personalization of smartcard token 400.

In step 905, the private keys are stored in memory 410. In step 906, any instance of the private key at the hardware security module or elsewhere in the initialization system is destroyed. This ensures that the only instance of the subscriber's private key is securely stored on smartcard token 400. Smartcard token 400 is preferably adapted to prevent any export of either private key from smartcard token 400.

In step 907, any desired additional software and data are loaded onto smartcard token 400. In step 908, issuing participant 102 binds subscribing customer 106 to smartcard token 400, as described above. In step 909, issuing participant physically issues smartcard token 400 and subscribing customer 106's digital certificate to subscribing customer 106, as described above.

FIG. 10 illustrates a preferred embodiment of a process for signing a message using the subscribing customer's smartcard token 400. As shown in FIG. 10, in step 1001, subscribing customer 106 visits relying customer 108's Web site. The parties preferably authenticate themselves over an SSL session using their utility keys. In step 1002, relying customer 108, via its Web server 220, sends subscribing customer 106 a message requesting that the subscribing customer digitally sign certain data (e.g., a purchase order for an agreed-to transaction).

In step 1003, subscribing customer 106's Web browser 224 transmits the data to be signed to smartcard subsystem 226. In step 1004, smartcard subsystem 226 prompts subscribing customer 106 for his or her PIN/passphrase. As discussed above, subscribing customer 106 preferably must enter his or her PIN/passphrase each time a signature is to be executed using the identity private key. In step 1005, subscribing customer 106 submits his or her PIN/passphrase to smartcard subsystem 226. In step 1006, if subscribing customer 106 enters the correct PIN/passphrase, smartcard token 400 unlocks the identity private key. If subscribing customer 106 enters an incorrect PIN/passphrase, he or she is prompted to re-

enter that information. If subscribing customer 106 exceeds the limit on the number of incorrect attempts to enter his or her PIN/passphrase, then smartcard token 400 is preferably blocked, as described above.

In step 1007, if the identity private key is unlocked, signature generator 424 uses the identity private key to sign the data to be signed. If CSSD is implemented, then CSSD generator 426 generates CSSD. In a preferred embodiment, subscribing customer 106 need not provide a PIN/passphrase in order to generate CSSD. CSSD is preferably automatically generated and included in the signed data by smartcard token 400. In step 1008, smartcard subsystem 226 transmits the signed data to Web browser 224. In step 1009, Web browser 224 transmits the signed data to Web server 220 for further four-corner processing.

In an alternative embodiment, subscribing customer may be provided with a signing interface to facilitate digital signing of messages by smartcard subsystem 226. An exemplary signing interface is described in U.S. provisional application serial No. 60/224,994, entitled Signing Interface Requirements, Hardware Compliance Requirements, Warranty Service Functional Requirements, and Additional Disclosure, filed August 14, 2000, which is hereby incorporated by reference.

In a preferred embodiment, some or all of the requirements described above may be weighted to enable an issuing participant to formulate a matrix to aid in evaluating the ability of potential vendors to meet the requirements. In this preferred embodiment, each weighted requirement to be satisfied by the vendor is scored by the issuing participant. The score assigned to a vendor for a given requirement is preferably based on their ability to satisfy the requirement functionally, technically, and with good quality.

Next, the score assigned by the issuing participant is multiplied by the requirement's weight and entered in the matrix. For example, if an issuing participant gave a vendor a score of eight for a given requirement, and the weight assigned the requirement was 10, then the number entered in the matrix would be 80. Totals for all requirements may be calculated and used in choosing an appropriate vendor. A preferred embodiment of weights assigned to particular requirements described above is shown in FIG. 11.

While the invention has been described in conjunction with specific embodiments, it is evident that numerous alternatives, modifications, and variations will be apparent to those skilled in the art in light of the foregoing description.